IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

ANDREA LARSON, on behalf of herself and all others similarly situated, Plaintiff, v. BELK, INC., Defendant.	Case No. 3:25-cv-00424 Class Action Jury Trial Demanded

AMENDED CLASS ACTION COMPLAINT

Plaintiff Andrea Larson ("Plaintiff"), through her attorneys, bring this Class Action Complaint against Defendant Belk Inc. ("Belk" or "Defendant"), alleging as follows:

I. INTRODUCTION

1. Belk is a retail company based in Charlotte, North Carolina, in operation for over 135 years with about 300 stores across 16 states and an annual revenue exceeding $3.3 billion.

2. This action arises from a cyberattack on Defendant's vulnerable information systems in which the personally identifiable information ("PII") of at least its employees were exposed to cybercriminals and identity thieves whose mission it is to use that information for identity theft and fraud operations (the "Data Breach").

3. On information and belief, and because of the types of information Belk collected on its employees, the Data Breach included Plaintiff's and the proposed Class Members' Social Security numbers, which is a critical component of criminal identity theft and fraud operations and the exposure of which places Plaintiff and the proposed Class at a serious and significant risk of identity theft and fraud for years to come.

4. Though Defendant maintain its systems in a vulnerable state, it represented that it

understood the importance of cybersecurity: "We understand the importance of security, the use of Secure Sockets Layer (SSL) – the industry standard for Internet Commerce transaction security – to encrypt your credit & personal information as it travels across the Internet to our secure services."[1]

5. Moreover, in its privacy policy, Defendant Belk further represents that it employed reasonable cybersecurity safeguards:

> We use commercially reasonable physical, technical, and administrative safeguards to assist us in preventing unauthorized access, use and disclosure of your personal information. However, because no measure is ever 100% effective, we do not guarantee that your personal information will be secure from theft, loss, or unauthorized access or use, and we make no representation as to the reasonableness, efficacy, or appropriateness of the measures we use to safeguard such data.[2]

6. Thus, though Belk attempts to hedge by noting that no system can be completely secure, it still attempts to draw its customers and employees into believing that Belk can be trusted with sensitive PII.

7. Notwithstanding these representations, and the ubiquitous nature of data breaches, Defendant Belk failed to reasonably secure its information systems from the well-known risk of cyberattacks targeting PII, such as this one.

8. According to Defendant's filing with the New Hampshire Attorney General's Office, hackers gained access to its information systems at least between May 7 and May 11, 2025 and stole files, including files containing Social Security numbers.[3]

9. On information and belief, the Data Breach occurred because Defendant maintain its information systems in a vulnerable state, including by not masking or encrypting Social

[1] https://www.belk.com/customer-service/policies-guidelines/ (last visited June 17, 2025).
[2] https://www.belk.com/customer-service/policies-guidelines/privacy-policy/ (last visited June 17, 2025).
[3] https://mm.nh.gov/files/uploads/doj/remote-docs/belk-20250605.pdf.

Security numbers and by failing to have systems in place sufficient to detect unauthorized intrusion or at least sufficient to detect when unauthorized third parties were downloaded these highly confidential files from Defendant's systems.

10. Defendant's failures and decisions to forego appropriate investments in cybersecurity safeguards has caused a severe invasion of privacy to Plaintiff and the proposed Class and forces them to face years of identity theft and fraud.

II. PARTIES

11. Plaintiff is a natural person and citizen of South Carolina, where she intends to remain.

12. Defendant Belk, Inc. is a Delaware corporation with its principal place of business at 2801 W. Tyvola Road, Charlotte, North Carolina, 28217.

III. JURISDICTION & VENUE

13. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least Plaintiff is a citizen of a state different from Defendant.

14. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

15. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

IV. BACKGROUND FACTS

16. Defendant collected the PII of Plaintiff and the proposed Class Members, which it

held and continues to hold unencrypted in its information systems.

17. Defendant made implicit promises to Plaintiff and Class Members that her PII would be kept safe and confidential, and that the privacy of that information would be maintained. Indeed, maintaining the confidences of customer and employee Social Security numbers is so fundamentally expected that it is implicit in every relationship that includes the sharing of such confidential information.

18. Plaintiff's and Class Members' PII was provided to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

19. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

20. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), industry standards, and representations made to Plaintiff and Class Members, to keep her PII confidential and to protect it from unauthorized access and disclosure.

21. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

22. On information and belief, Plaintiff's information was included because she is a former employee and the Data Breach appears to be so widespread as to include Social Security numbers, which Defendant Belk collects on employees but has no known reason to collect from its retail customers.

Defendant's Data Breach Was Imminently Foreseeable

23. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PII, like Defendant, preceding the date of the Data Breach.

24. Data thieves regularly target institutions like Defendant due to the highly sensitive information in her custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

25. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[4]

26. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members because of a breach.

27. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

28. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially tens of thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

29. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of

[4] *See* Identity Theft Res. Ctr., *2021 Data Breach Annual Report*, at 6 (Jan. 2022), https://notified.idtheftcenter.org/s/.

Plaintiff and Class Members.

30. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Personally Identifiable Information

31. Identity theft is "a fraud committed or attempted using the identifying information of another person without authority."[5] It is described as "identifying information" such as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[6]

32. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[7]

33. For example, PII can be sold at a price ranging from $40 to $200.[8] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[9]

34. Based on the foregoing, the information compromised in the Data Breach is even more significant because it includes Social Security numbers, which is significantly difficult if not

---

[5] 17 C.F.R. § 248.201 (2013).
[6] *Id.*
[7] Anita George, *Your Personal Data Is for Sale on The Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.
[8] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.
[9] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark.

impossible to change.

35. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[10]

36. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

Defendant Failed to Comply with FTC Guidelines

37. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

38. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines

[10] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.
[11] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand her network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

39. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

40. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet her data security obligations.

41. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

42. Defendant was at all times fully aware of its obligation to protect the PII of consumers under the FTC Act yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

43. Moreover, by reviewing the consent decrees the FTC has entered into with the companies after data breaches, companies should be able to easily see what standards and safeguards the FTC believes are mandatory to have a cybersecurity program that is appropriate and avoids amounting to a deceptive or unfair practice. These consent orders/decrees have been termed a sort of common law of cybersecurity safeguards, establishing a clearly defined standard of care for companies to follow.[12]

Defendant Failed to Comply with Industry Standards.

44. Experts studying cybersecurity routinely identify institutions that store PII like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

45. Some industry best practices that should be implemented by institutions dealing with sensitive PII, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its timeline,

[12] *See generally* Woodrow Hertzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 George Wash. L.R. 2230 (2015).

Defendant failed to follow some or all these industry best practices.

46. Other best cybersecurity practices that are standard at large institutions that store PII include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

47. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

48. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Common Injuries & Damages

49. Because of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); and (d) the continued risk to her PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and

adequate measures to protect Plaintiff's and Class Members' PII.

The Data Breach Increases Victims' Risk of Identity Theft.

50. Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because Defendant's failures resulted in Plaintiff's and Class Members' Social Security number falling into the hands of identity thieves.

51. The unencrypted PII of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the PII for the express purpose of conducting financial fraud and identity theft operations.

52. Further, the standard operating procedure for cybercriminals is to use some data, like the Social Security numbers here, to access "fullz packages" of that person to gain access to the full suite of additional PII that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.[13]

53. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to

[13] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

54. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

55. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that her PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendant arguing that the individual failed to mitigate damages.

56. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff's and Class Members' Social Security numbers or other government identification are affected.

57. By spending this time, data breach Plaintiff was not manufacturing her own harm, she was taking necessary steps at Defendant's direction and because the Data Breach included her Social Security number.

58. Plaintiff and Class Members have spent, and will spend additional time in the

future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on her accounts; changing passwords and re-securing her own computer networks; and checking her financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

59. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to her good name and credit record."[14]

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

60. Based on the value of the information stolen, the data either has or will be sold to cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

61. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

62. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for

[14] *See* U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

Defendant's failure to safeguard her PII.

Plaintiff's Experience

63. Plaintiff is a former employee of Defendant from 2019 to 2021.

64. Plaintiff's PII remained in Defendant's information system and was stolen by cybercriminals along with the data of the other current and former employees of Defendant—and potentially its customers.

65. Plaintiff's PII was compromised in the Data Breach and stolen by identity thieves who illegally accessed Defendant's network for the specific purpose of targeting the PII.

66. Plaintiff takes reasonable measures to protect her PII.

67. Plaintiff suffered actual injury in the form of a severe privacy invasion because of her PII, including her Social Security number, falling into the hands of identity thieves whose mission it is to use that information to perpetrate identity theft and financial fraud.

68. Plaintiff suffered lost time, interference, and inconvenience because of the Data Breach and has experienced stress and anxiety due to increased concerns for the loss of her privacy and because she that knows she must now face a substantial increase in identity theft and financial fraud attempts for years to come.

69. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her name and Social Security number, being placed in the hands of criminals whose mission it is to misuse that data.

70. Indeed, Plaintiff now receives a significant amount of spam and phishing messages, including messages.

71. Moreover, Plaintiff has been alerted to malicious attempts to access her Paypal

account.

72. Alarmingly, Plaintiff has also been getting messages that someone is trying to access her Coinbase account, but she never opened an account with Coinbase and still does not do business with that company.

73. Defendant obtained and continues to maintain Plaintiff's PII and thus has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Furthermore, because Defendant still maintains Plaintiff's information in a vulnerable state, Plaintiff has standing to seek injunctive relief requiring Defendant to implement reasonable cybersecurity safeguards to protect her PII.

74. Because of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ACTION ALLEGATIONS

75. Plaintiff sues on behalf of herself and the proposed Class ("Class"), defined as follows:

> All individuals whose PII was compromised in the Data Breach affecting Defendant.

76. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

77. Plaintiff reserves the right to amend the class definition.

78. This action satisfies the requirements of Federal Rule of Civil Procedure 23.

a. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of far too many members to join in a single action—while the precise number of total breach victims is unknown, on information and belief, the Data Breach has impacted at least tens of thousands of former and current employees;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with Class members' interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common factual and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. If Defendant had a duty to use reasonable care in safeguarding Plaintiff and the Class's PII;

ii. If Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. If Defendant was negligent in maintaining, protecting, and securing PII;

iv. If Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

v. If the Data Breach injured Plaintiff and the Class;

vi. What the proper damages measure is; and

vii. If Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

79. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiff are insufficient to make individual lawsuits economically feasible.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

80. Plaintiff incorporates the above allegations as if fully set forth herein.

81. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that happened, and to promptly detect attempts at unauthorized access.

82. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with reasonable industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately happened. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by

disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

83. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

84. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff and members of the Class's personal information and PII.

85. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

86. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class's and the importance of exercising reasonable care in handling it.

87. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal

information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

88. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CLAIM FOR RELIEF
Negligence Per Se
(On Behalf of Plaintiff and the Class)

89. Plaintiff incorporates the above allegations as if fully set forth herein.

90. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

91. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Defendant, of failing to use reasonable measures to protect customers or, in this case, customers' PII. The FTC publications and orders promulgated under the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

92. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result in the event of a breach, which ultimately came to pass.

93. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

94. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

95. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

96. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

97. Indeed, the FTC Act provides a comprehensive and known set of requirements for the implementation of reasonable cybersecurity through its guidance materials and through its consent orders following data breach investigations. These consent orders have been called a sort

of common law of FTC requirements and clearly establish the expected measures necessary to comply with the FTC Act.

98. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

99. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

100. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

101. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

102. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

103. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

104. Plaintiff incorporates the above allegations as if fully set forth herein.

105. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

106. Defendant owed a duty to its customers, including Plaintiff and the Class, to keep this information confidential.

107. The unauthorized acquisition (*i.e.,* theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

108. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

109. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

110. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

111. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

112. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

113. Moreover, the definition of intent is met here under Section 8A of the Restatement (Second) of Torts in that, given the ubiquity of data breaches, Defendant was substantially certain that its decision to forego the appropriate investments in cybersecurity defense measures would lead to a data breach.

114. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

115. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

116. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

117. Plaintiff incorporates the above allegations as if fully set forth herein.

118. This claim is pled in the alternative pursuant to Rule 8.

119. Plaintiff and members of the Class conferred benefits upon Defendant in the form their PII and their employment services, which Plaintiff would not have conveyed if she knew of Defendant's poor cybersecurity practices.

120. Defendant appreciated or knew of these benefits that it received. And under principles of equity and good conscience, this court should not allow Defendant to retain the full value of these benefits—specifically, the money Defendant saved by foregoing the proper

investments in cybersecurity.

121. After all, Defendant failed to adequately protect their PII. And if such inadequacies were known, then Plaintiff and the members of the class would never have conferred benefits nor disclosed their PII.

122. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and members of the Class—all funds that were unlawfully or inequitably gained despite Defendant's misconduct and the resulting Data Breach.

FIFTH CLAIM FOR RELIEF
North Carolina Unfair and Deceptive Trade Practices Act
(On Behalf of Plaintiff and the Class)

123. Plaintiff incorporates the above allegations as if fully set forth herein.

124. Defendant advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

125. Such commerce was only possible because of and included Plaintiff's employment.

126. Defendant engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures—which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII—including duties imposed by

the FTC Act—which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act.

127. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

128. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

129. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Still, Defendant accepted the PII that Plaintiff and Class Members entrusted to it—while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

130. Defendant acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair and Deceptive Trade Practices Act. Moreover, Defendant recklessly disregarded Plaintiff's and Class members' rights.

131. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury,

ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

132. Defendant's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses under N.C. Gen. Stat. Ann. § 75-8.

133. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

VI. PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

VII. JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: June 20, 2025

Respectfully submitted,

/s/ Scott C. Harris

Scott C. Harris (NC Bar No. 35328)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W. Morgan Street
Raleigh, NC 27603
Tel: (919) 600-5003
sharris@milberg.com

J. Gerard Stranch, IV*
Grayson Wells*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

* *Pro hac vice forthcoming*

Counsel for Plaintiff and the Proposed Class